On-Line Privacy

A Selection of Current Law, Cases, and Legislation

United States

California

European Union

Prepared By: *Lynn M. Holmes, Esquire*
Attorney & Counselor-At-Law
PO Box 207, Forestville, CA 95436
Phone 707-887-9399
E-mail: lynn.holmes@usa.net

Last Updated: June 2, 2000

To obtain additional copies please contact the author:
Lynn M. Holmes, Esquire – PO Box 207, Forestville, CA 95436,
Phone: 707-887-9399, Fax: 707-887-8387 E-Mail: lynn.holmes@usa.net

Table of Contents

I. Federal – Existing Law I-1

A. Children's Online Privacy Act of 1998 (COPPA) I-1

1. General Provisions – 16 CFR Part 312. ..... I-1

B. Gramm-Leach-Bliley Act (P.L. 106-102) I-3

1. Notices of the institutions privacy practices and policies: I-4
2. Online / Internet Requirements of the Rule: I-4

C. National Labor Relations Act (NLRA Act) I-6

D. FTC Internet Privacy Actions I-7

1. GeoCities, Inc., Aug 1998 ..... I-7
2. Liberty Financial Companies, Inc. (younginvestor.com), May 1999 ..... I-7
3. ReverseAuction.Com, Jan. 2000 ..... I-8
4. DoubleClick, Inc. I-8

II. California – Existing Law II-10

A. Information Practices Act of 1977 ..... II-10

B. California Public Records Act. II-10

III. Proposed Rules and Legislation III-11

A. Federal III-11

1. HR 3560 Online Privacy Protection Act of 2000 ..... III-11
2. S854 Electronic Rights for the 21st Century Act III-11
3. HR 1685 Internet Growth and Development Act of 1999 ..... III-12
4. Additional Legislation Being Considered Pertaining to Internet Privacy III-13

B. State of California – III-14

1. AB 1793 Internet Privacy Protection Act Of 2000 ..... III-14
2. SB 129 Personal Information: Collection and Disclosure III-14
3. AB 1707 Consumers' Financial Privacy Act. III-15

.
.
.
4. SB 1409 California Privacy Protection Act of 2000 ..... III-15
5. SB 1599 Privacy: In Home Television Services III-15

IV. European Union IV-16

A. European Union (EU) Directive on the Protection of Personal Data IV-16

I. Federal – Existing Law

A. Children's Online Privacy Act of 1998 (COPPA)

15 U.S.C. 6501, et seq.

Federal Trade Commission (FTC) Rule1: 16 CFR Part 312 Effective April 21, 2000.

This Act protects children's privacy by giving parents the tools to control what information is collected from their children online. Under the Act's implementing Rule (codified at 16 C.F.R. Part 312), operators of commercial websites and online services directed to or knowingly collecting personal information from children under 13 must:

- notify parents of their information practices;
- obtain verifiable parental consent before collecting a child's personal information;
- give parents a choice as to whether their child's information will be disclosed to third parties;
- provide parents access to their child's information;
- let parents prevent further use of collected information;
- not require a child to provide more information than is reasonably necessary to participate in an activity; and
- maintain the confidentiality, security, and integrity of the information.

1. General Provisions – 16 CFR Part 312.

a) Personal Information

Definition includes: a first and last name, a home or other physical address, an e-mail address or other online contact information, including but not limited to an instant messaging user identifier or a screen name that reveals an individual's e-mail address, a telephone number, a social security number, a persistent identifier such as a customer number held in a cookie or a processor serial number, where such identifier is associated with individually identifiable information, or information concerning the child or parents of that child that the operator collects online from the child and combines with an identifier described in this definition. §312.2(a)-(g).

b) Privacy Notice on The Web Site §312.3(a)

An operator who collects any personal information from a child must provide notice on the web site or the online service of what information it collects from children, how it

[1] Copies of all FTC Rules and comments are available at www.ftc.gov. The website home page includes a link to the FTC Privacy Initiatives page.

uses such information, and its disclosure practices for such information. This notice must comply with §312.4(b), which requires:

- notices to be clearly and understandably written, be complete, and must contain no unrelated, confusing of contradictory materials;
- a link to a notice of its information practices on its homepage and at each area on the website or online service where personal information is collected from children;
- the link must be in a clear and prominent place in each required area;
- the notice must state the name, address, telephone number, and e-mail address of all operators collecting or maintaining personal information from children through the web site or online service;
- the notice must state the types of personal information and whether it is collected passively (i.e., through cookies) or directly;
- how the personal information is to be used by the operator; and
- whether the information is disclosed to third parties, the nature of the third parties business, whether the third party has agreed to maintain confidentiality, security and integrity of the personal information; and
- procedures and methods for parents to review, delete and refuse to permit further collection or use of the child's information.

c) Verifiable Parental Consent §312.5

An operator must make reasonable efforts to obtain verifiable parental consent, taking into account available technology.

Methods to obtain verifiable parental consent include:

A written consent form signed by the parent and returned via fax or postal mail, use of a credit card in connection with a transaction, having a parent call a toll free number staffed by trained personnel, using a digital certificate that uses public key technology, or using e-mail accompanied by a PIN or password obtained through one of the other verification methods.

d) Choice Regarding Disclosures to Third Parties

Parents have the option to consent to the collection and use of their child's personal information without consenting to the disclosure of information to third parties. §312.4(b)(vi). Also, see §312.6

e) Online Activities for Which Parental Control Is Not Required

§312.5(c) provides exceptions to prior parental consent::

- where the sole purpose of collecting the name or online contact information is to obtain parental consent or providing notice under §312.4;
- where the operator is responding to a one time request to a specific request from a child;
- where the personal information collected is not used by the operator for any other purpose than responding directly to a specific request of the child; or
- where the operator collects personal information to extent reasonably necessary to protect the safety of a child participant on the website

f) Coverage of Information Submitted Online

The Federal Register notice accompanying the rule makes clear that the rule covers only information submitted online, and not information requested online but submitted offline.

g) Role of Schools in Obtaining Consent of Students

The Federal Register notice accompanying the rule makes clear that schools can act as parents' agents or as intermediaries between web sites and parents in the notice and consent process.

h) Safe Harbor Program

In order to encourage active industry self-regulation, the Act also includes a "safe harbor" provision allowing industry groups and others to request Commission approval of self-regulatory guidelines to govern participating websites' compliance with the Rule.

B. Gramm-Leach-Bliley Act (P.L. 106-102)

FTC Final Rule[2]: Privacy of Consumer Financial Information

[2] Complete copies of the Rule and comments can be found at www.ftc.gov

16 CFR Part 313 Effective November 13, 2000. Requires full compliance by financial institutions by July 1, 2001

The purpose of the Gramm-Leach-Bliley Act (G-L-B Act) is to enable an individual to limit the sharing of non-public in formation by a financial institution with a non-affiliated third party. The G-L-B Act requires financial institutions as defined by section 4(k) of the Bank Holding Company Act, to offer consumers and customers the opportunity to "opt-out" of the transmission of non-public personal information by the institution to non-affiliated parties. [3]

Sec 503(a) requires a financial institution to disclose its policies and practices with respect to sharing information both with affiliated and non-affiliated third parties to customers. The rules promulgated by the Federal Trade Commission (FTC) (16 CFR Part 313) applies only to information about individuals who obtain a financial product or service from a financial institution to be used for personal, family, or household purposes.[4]

1. **Notices of the institutions privacy practices and policies:**
   a) must be made at the time of establishing a customer relationship with the individual and thereafter, as long as the relationship continuers, on an annual basis to all customers[5];
   b) notice to consumers, who are not customers, must be made prior to disclosing non-public personal information to a non-affiliated third party, §313.4(a)(2);
   c) accurately reflect the institutions privacy practices and policies, 16 CFR §313.6(a)(8);
   d) must be clear and conspicuous, 16 CFR 313.3(b)(1), and
   e) include a description of the opt-out rights and methods to opt-out that are available to the customer. 16 CFR 313.6(a)(6).

2. **Online / Internet Requirements of the Rule:**
   a) Disclosures on Web Pages:
   § 313.3(b)(2)(iii) provides that may be found to comply with the rule that they be "clear and conspicuous", if they use text or visual cues to encourage scrolling to view the entire notice and ensure that other elements of the web page do not distract attention

[3] 16 CFR §313.1 Purpose and Scope;
[4] Id.
[5] 16 CFR §313.4(a)(1) Initial notice to consumers required; §313.5(a)(1) Annual notice to customers required; General rule.

away from the notice. The financial institution must also place a notice of conspicuous link on a page frequently accessed by consumers, such as the page on which transactions are conducted.[6]

The financial institution must also place a notice of conspicuous link on a page frequently accessed by consumers, such as the page on which transactions are conducted.[7]

b) Online Institutions:

Institutions operating online, as well as those operating offline, will have to evaluate whether they are required to make disclosures, including (1) whether they are engaged in a financial activity, and (2) if so, whether they have consumers or customers that trigger the disclosure or other requirements of the act.

The FTC notes that one of the financial activities incorporated by reference into Sec. 4(k) of the Bank Holding Company Act is:

> "providing data processing and data transmission services, facilities (including data processing and data transmission hardware, software, documentation, or operating personnel), data bases, advice, and access to such services, facilities, or data bases by any technological means, if…[t]he data to be processed or furnished are financial, banking, or economic…"

12 CFR § 225.28(b)(14).[8] Some financial software and hardware manufacturers, as described at may find themselves classified as financial institutions. However, if these manufacturers only sell to businesses they will have no disclosure obligations. In addition, this language, according to the FTC supplemental information brings into the definition of financial institution Internet companies that provide an individual with access via the company's web site, to the individual's financial accounts (such as credit cards, mortgages, and loans) by compiling, or aggregating the individual's on-line financial accounts.[9]

---

[6] FTC supplementary information report to final privacy rule, 16 CFR 313: Privacy of Consumer Financial Information, Page 15-16, and 16 CFR 313.3(b)(1) – 313.3(b)(2)(iii)

[7] FTC supplementary information report to final privacy rule, 16 CFR 313: Privacy of Consumer Financial Information, Page 15-16, and 16 CFR 313.3(b)(1) – 313.3(b)(2)(iii)

[8] Id., Page 36.

[9] Id., Page 36.

c) Delivering privacy and opt out notices

Each customer can reasonably be expected to receive actual notice in writing, or, if the consumer agrees, electronically. 16 CFR §313.9(a) How to provide notices. It can be reasonably expected that a consumer who conducts transactions electronically, will have been given actual notice if a clearly and conspicuously posted notice is on the electronic site, and the consumer is required to acknowledge receipt of the notice as a necessary step of obtaining the particular financial product or service. 16 CFR §313.0(a)(b)(1)(iii).

C. National Labor Relations Act (NLRA Act)

Many companies have policies restricting the use of company e-mail systems to business communications. Courts have generally held that since employers own the computers and the networks on which e-mail is facilitated, they are free to monitor, intercept, read, and to set the rules for use and the ramifications for misuse. Employees have no privacy rights in e-mail sent through a company e-mail system.

However, taking a different cause of action, "unfair labor practices", two recent cases e-mail messages that the company found to be in violation of company e-mail policy and used as a basis to take disciplinary action against employees, found the e-mail to be "concerted activities" and protected by the NLRA Act. The of e-mails were used to communicate about work terms and conditions. Thus, a complete ban is not always possible. The cases that lend some guidance as to when an employer can ban all non-business use and discipline employees based on the content of monitored e-mail.[10]

1. NLRB v. Timekeeping Systems, 323 NLRB No. 30, Feb. 1997

In the NRLB's first ruling that the use of e-mail is protected when it is used by nonsupervisory workers to communicate with other employees in an effort to influence working conditions occurred in 1997. The NLRB concluded that the Timekeeping Systems, Inc. violated §8(a)(1) of the NLRB Act by discharging the employee, Larry Leinweber, for an e-mail that was transmitted to other employees and was, in and of itself , "concerted activity" within the meaning of the NLRB Act.

2. NLRB v. Pratt & Whitney – Advisory Memo

[10] Michael J, McCarthy, Wall Street Journal, *Workers new tool in privacy revolt*, as published in the San Francisco Examiner, Page J-1, May 21, 2000

An employee of Pratt & Whitney, Brian Waldron, was suspended for one month without pay, in June 1997, after having "been warned, suspended or otherwise disciplined" for using e-mail for union messages or because employees have downloaded information from the union's Web page onto company computers. Pratt & Whitney had a policy in place that banned the use of company computers and e-mail for all non-business uses.

The NRLB's general office issued an advisory memo stating that a company cannot issue a complete ban on all e-mail, which necessarily includes employee's messages otherwise protected by federal law. The memo included the analogy that e-mail was more like a telephone call than mail, as it allows the reader to talk back. The ability to exchange ideas and discuss what action to collectively take is the key to effective preservation of labor rights and the equalization of bargaining power.

While the advisory memo is not precedent, it does provide guidance to companies as they establish and review e-mail policies. Pratt & Whitney later changed the e-mail policy to allow for occasional personal use of company e-mail and to allow for discussions relating to the "terms and conditions of employment and the employee's interest in self-organization."

D. FTC Internet Privacy Actions

1. GeoCities, Inc., Aug 1998[11]

GeoCities agreed to settle FTC charges that it misrepresented the purposes for which it was collecting personal identifying information from children and adults. This is the first FTC case involving Internet privacy. The case was settled before the COPPA rules implementation. Under the settlement, GeoCities agreed to post on its site a clear and prominent Privacy Notice, telling consumers what information is being collected and for what purpose, to whom it will be disclosed, and how consumers can access and remove the information. To ensure parental control, GeoCities also would have to obtain parental consent before collecting information from children 12 and under.

2. Liberty Financial Companies, Inc. (younginvestor.com), May 1999[12]

[11] Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case: Commission Establishes Strong Mechanisms for Protecting Consumers' Privacy Online, Aug. 13, 1998, http://www.ftc.gov/opa/1998/9808/geocitie.htm

Addressing children's online privacy prior to COPPA, the FTC settled with Liberty Financial Companies, Inc., the operator of the Young Investor website. The Young Investor website is directed to children and teens, and focuses on issues relating to money and investing. The Commission alleged that the site falsely represented that personal information collected from children in a survey would be maintained anonymously, and that participants would be sent an e-mail newsletter as well as prizes. In fact, the personal information about the child and the family's finances was maintained in an identifiable manner. The consent agreement prohibits such misrepresentations in the future and would require Liberty Financial to post a privacy notice on its children's sites and obtain verifiable parental consent before collecting personal identifying information from children.

3. ReverseAuction.Com, Jan. 2000[13]

Online auction house ReverseAuction.com, Inc. agreed to settle FTC charges that it violated consumers' privacy by harvesting consumers' personal information from eBay's site and then sending deceptive spam to those consumers soliciting their business. Settlement of the FTC charges bar ReverseAuction from engaging in such unlawful practices in the future. It also requires ReverseAuction to delete the personal information of consumers who received the spam but declined to register with ReverseAuction; and to give those who did register, as a result of the spam, notice of the FTC charges and an opportunity to cancel their registration and have their personal information deleted from ReverseAuction's database.

4. DoubleClick, Inc.

On February 10, 2000, a complaint[14] was filed with the FTC alleging that the FTC notified us that they were conducting an informal inquiry into our business practices to determine whether, in collecting and maintaining information concerning Internet users, we have engaged in unfair or deceptive practices.

The complaint rises from the earlier purchase of Abacus Direct Corp. by DoubleClick. Abacus maintains one of the largest offline catalog databases in the country. DoubleClick proposed

---

[12] Young Investor Website Settles FTC Charges: Agency Alleged Website Made False Promises About Collection of Personal Information from Children and Teens, May 6, 1999, http://www.ftc.gov/opa/1999/9905/younginvestor.htm

[13] Online Auction Site Settles FTC Privacy Charges: Personal Identifying Information Hijacked From Competitor's Site; Many Consumers Sent Deceptive Spam, Jan. 6, 2000, http://www.ftc.gov/opa/2000/01/reverse4.htm

[14] Copies of the complaint can be found at www.epic.org/privacy/internet/ftc/CLK_complaint.pdf

linking the anonymous Internet profiles in the DoubleClick database with the personal information contained in the Abacus database.

The complaint alleges that the merger of the databases violates DoubleClick's assurances to Internet users that the information it collects through their online activities will remain anonymous, and that the data collection is therefore unfair and deceptive.

DoubleClick also faces suits in various jurisdictions[15]:

- Judnick v. DoubleClick, Inc., Jan. 2000, was filed against us in the Superior Court of the State of California, in Marin County. The complaint alleges that DoubleClick engaged in unfair business practices and false and misleading advertising in violation of certain California consumer protection statutes by allegedly improperly collecting and utilizing information about Internet users.
- Bruce v. DoubleClick, Inc. , Jan. 2000, was filed against us in the U.S. District Court for the Northern District of California. The complaint alleges that we have improperly collected and used Internet users' information, allegedly in violation of certain federal electronics privacy statutes and common law privacy rights.
- Steinbeck v. DoubleClick, Inc., Jan. 2000, was filed in the United States District Court for the Central District of California. The complaint alleges that we engaged in unlawful business practices by improperly obtaining and using information about Internet users allegedly in violation of federal statutes and Internet users' privacy rights.
- DeCorse v. DoubleClick, Inc, Jan. 2000 was filed in the Superior Court of the State of California, Marin County. The complaint alleges that we engaged in unlawful business practices by improperly obtaining and using information about Internet users allegedly in violation of California statutory and common law.
- Healy v. DoubleClick Inc., Jan. 2000, was filed against us in the U.S. District Court for the Southern District of New York. The complaint alleges that we improperly collected and used information concerning Internet users allegedly in violation of certain federal electronics privacy statutes, as well as common law trespass and invasion of privacy
- Donaldson v. DoubleClick Inc., Feb. 2000, was filed against us in the U.S. District Court for the Southern District of New York. The complaint alleges that we improperly collected and used information concerning Internet users allegedly in violation of certain federal electronics privacy statutes and common law privacy rights.

[15] DoubleClick, Inc., February 14, 2000 SEC Edgar filing.

II. California – Existing Law

A. Information Practices Act of 1977[16]

Requires state and local agencies, among other things, to maintain in its records only that personal information, as defined,

- which is relevant and necessary to its governmental purpose;
- to maintain its sources of information;
- to maintain accurate, relevant, and complete records;
- to disclose personal information only under specified circumstances;
- to maintain records regarding the disclosure of personal information; and
- to allow individuals access to those records pertaining to them, except as specified, to provide for the amendment of those records.

The act also establishes civil remedies for its enforcement. §1798.53 provides for a civil cause of action

B. California Public Records Act.

Public Records Act, Govt. Code §6250 et seq., governs public access to records maintained by state and local public agencies.

6250. In enacting this chapter, the Legislature, mindful of the right of individuals to privacy, finds and declares that access to information concerning the conduct of the people's business is a fundamental and necessary right of every person in this state.

6254.21. (a) No state or local agency shall post the home address or telephone number of any elected or appointed official on the Internet without first obtaining the written permission of that individual.

[16] CALIFORNIA CODES CIVIL CODE § 1798 - 1798.1

1798. This chapter shall be known and may be cited as the Information Practices Act of 1977.

1798.1. The Legislature declares that the right to privacy is a personal and fundamental right protected by Section 1 of Article I of the Constitution of California and by the United States Constitution and that, all individuals have a right of privacy in information pertaining to them. The Legislature further makes the following findings:

(a) The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies.

(b) The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information.

III. Proposed Rules and Legislation

A. Federal

1. HR 3560 Online Privacy Protection Act of 2000[17]

Related Senate Bill: S 809 Online Privacy Protection Act of 1999

"To require the Federal Trade Commission to prescribe regulations to protect the privacy of personal information collected from and about individuals who are not covered by the Children's Online Privacy Protection Act of 1998 on the Internet, to provide greater individual control over the collection and use of that information, and for other purposes."[18]

Online Privacy Protection Act of 2000 - Makes it unlawful for an operator of a Web site or online service to collect, use, or disclose personal information concerning an individual (age 13 and above) in a manner that violates regulations to be prescribed by the FTC. Such operators would be required to protect the confidentiality, security, and integrity of personal information it collects from such individuals. Requires such regulations to require such operators to provide a process for such individuals to consent to or limit the disclosure of such information.

Authorizes the States to enforce such regulations by bringing actions on behalf of residents, requiring the State attorney general to first notify the FTC of such action. Authorizes the FTC to intervene in any such action.

2. S854 Electronic Rights for the 21st Century Act

Title: A bill to protect the privacy and constitutional rights of Americans, to establish standards and procedures regarding law enforcement access to location information, decryption assistance for encrypted communications and stored electronic information, and other private information, to affirm the rights of Americans to use and sell encryption products as a tool for protecting their online privacy, and for other purposes.

Bill Table of Contents:

Title I: Privacy Protection for Communications and Electronic Information
Title II: Promoting Use of Encryption
Title III: Privacy Protection for Library Loan and Book Sale Records

[17] Short Title as introduced in the U.S. House of Representatives January 31, 2000. Sponsor: Rep. Rodney P. Frelinghuysen

[18] Official Title as introduced.

Title IV: Privacy Protection for Satellite Home Viewers

a) Title I: Privacy Protection for Communications and Electronic Information

Amends the Federal criminal code to authorize a governmental entity to require a provider of remote computing service to disclose the contents of any electronic communication made by subscribers only pursuant to a Federal or State warrant, or a Federal or State grand jury or trial subpoena.

(Sec. 106) Provides limited conditions under which a provider of domain name registration (a service which assigns and manages domain names and Internet addresses) may disclose a record or other information pertaining to a subscriber or customer of such service.

(Sec. 110) Provides limited conditions under which a provider of electronic communication or remote computing service may disclose a record or other information pertaining to a subscriber or customer to any persons other than a governmental entity.

b) Title II: Promoting Use of Encryption

Authorizes any person within the United States, and any U.S. person in a foreign country, to use, develop, manufacture, sell, distribute, or import any encryption (scrambling) product. Prohibits any U.S. agency from requiring, compelling, setting standards for, conditioning approval on, or conditioning the receipt of any benefit on a requirement that a decryption key (descrambler), access to a decryption key, key recovery information, or other plaintext access capability be: (1) required to be built into computer hardware or software for any purpose; (2) given to any other person; or (3) retained by any person using encryption.

3. HR 1685 Internet Growth and Development Act of 1999

Latest Major Action: 6/30/1999 House committee/subcommittee actions

Title: To provide for the recognition of electronic signatures for the conduct of interstate and foreign commerce, to restrict the transmission of certain electronic mail advertisements, to authorize the Federal Trade Commission to prescribe rules to protect the privacy of users of commercial Internet websites, to promote the rapid deployment of broadband Internet services, and for other purposes.

Bills Table of Contents:

Title I: Authorization of Electronic Signatures in Commerce

Title II: Electronic Mail Advertisements

Title III: Online Privacy Protection

Title IV: Broadband Deployment

Title V: Antitrust and Criminal Provisions

a) Title III: Online Privacy Protection

Requires any person operating a commercial Internet website to clearly and conspicuously provide notice of its collection, use, and disclosure policies concerning personally identifiable information. Provides for enforcement of such requirement under the Federal Trade Commission Act.

4. Additional Legislation Being Considered Pertaining to Internet Privacy

a) HR 313: Consumer Internet Privacy Protection Act of 1999

b) HR 2282: Internet Consumer Information Protection Act

c) HR 3221: Electronic Privacy Bill of Rights Act of 1999

d) S 1908: Student Privacy Protection Act (Introduced in the Senate)

HR 2915: Student Privacy Protection Act (Introduced in the House)

e) HR 3709: Internet Nondiscrimination Act of 2000

f) HR 3770: Secure Online Communication Enforcement Act of 2000

S 2063: Secure Online Communication Enforcement Act of 2000

g) S 759: Inbox Privacy Act of 1999

h) HR 3113: Unsolicited Electronic Mail Act of 1999

i) HR 2644: Personal Data Privacy Act of 1999

j) HR 3489: Wireless Telecommunications Sourcing and Privacy Act

k) HR 4246: Cyber Security Information Act

l) S 798: Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act of 1999

m) S 2430: Internet Security Act of 2000

n) HR 354: Collections of Information Antipiracy

o) S 736: Freedom From Restraint Act of 1999

p) HR 1858: Consumer and Investor Access to Information Act of 1999

q) HR 2616: Encryption for the National Interest Act

r) HR 850: Security And Freedom through Encryption (SAFE) Act

B. State of California[19] –

1. AB 1793 Internet Privacy Protection Act Of 2000

The April 27, 2000 amendment to this bill replaced the content with a single sentence statement of the California legislature's intent to enact legislation protecting the privacy of Internet users.

The IPPA Act states that:

> "The Legislature finds and declares that the privacy of internet users is increasingly at risk due to the widespread collection and distribution of personally identifying information for marketing and other purposes, and that this practice infringes on the fundamental right to privacy guaranteed to all citizens of California by the California Constitution. It is therefore the intent of the Legislature to enact legislation to protect the privacy of Internet users."

The office of the bill's author wishes to move the bill along and send it as a vehicle to the Internet privacy conference committees. It is the practice and custom of the state assembly to hold all "spot" [20] bills at the Assembly Rules Committee (ASM) until the bill is amended into a substantive form.[21]

2. SB 129 Personal Information: Collection and Disclosure

An act to add Title 1.81 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, and to add Article 6 (commencing with Section 12260) to Chapter 3 of Part 2 of Division 3 of Title 2 of the Government Code, relating to privacy.

As most recently amended on August 26, 1999 in the assembly this bill would:

Declare that any individual may sue a commercial or governmental agency for the unlawful disclosure of personal information about that individual without their permission.

Establishes a position of Privacy Ombudsman under the Secretary of State with the following responsibilities:

- Ensuring that commercial and governmental records are maintained such that personal information about individuals is not released in violation of law.

[19] The status and copies of the text of all bills before the California State Legislature can be found online at: www.leginfo.ca.gov

[20] Bills that do not contain substantive provisions are described as "spot" bills.

[21] AB1793 Assembly Bill – Analysis: ASSEMBLY COMMITTEE ON CONSUMER PROTECTION, GOVERNMENTAL EFFICIENCY, AND ECONOMIC DELVELOPMENT, May 2, 2000.

- Acting as a nonbinding arbiter in disputes regarding the unlawful release of personal information gathered by commercial or governmental entities.
- Recommending any corrections or changes to a commercial or governmental record pursuant to an administrative proceeding.
- Adopting any regulations necessary to implement the above requirements.
- Authorizes any commercial or governmental record holder found by the ombudsman to have unlawfully released personal information to seek redress in the courts.
- Creates a rebuttable presumption that the unlawful release of personal information results in damages and would provide that in a related cause of action damages shall be trebled under certain circumstances.

The bill has left some fundamental terms undefined, such as, "personal information", "person" and "commercial or governmental purpose".

3. AB 1707 Consumers' Financial Privacy Act.

An act to add Chapter 2 (commencing with Section 1798.80) to Title 1.8 of Part 4 of Division 3 of the Civil Code, relating to financial privacy.

This Act failed at the Assembly Banking and Finance Committee on April 24, 2000. It would have prohibited a financial institution from disclosing or making an unrelated use of a consumer's prior written consent, as specified.

4. SB 1409 California Privacy Protection Act of 2000

The bill would make it a crime for a consumer credit reporting agency, financial institution, health care provider, or insurance company to disclose to a third party or parties personal information relating to an individual without that individual's prior consent. The bill would also set forth various definitions and create a new cause of action for a violation. The bill would impose a state-mandated local program by creating a new crime.

5. SB 1599 Privacy: In Home Television Services[22]

An act to amend Section 637.5 of the Penal Code, relating to privacy.

This bill would amend the code to expand §637.5 requirements to all "video providers", rather than "cable television corporation". The bill imports the definition of video providers from the Cable Television and Video Provider Customer Service and Information Act.

[22] Introduced by Senator Bowen, February 18, 2000, Amended March 23, 2000.

Video Providers would include any provider utilizing the Internet to deliver television services over the Internet. This would include customized programming for individual subscribers and services such as WebTV.

§6375(a)(1) requires that a subscriber opt-in by requiring the video provider to obtain "the express written consent of the subscriber" to use any electronic device to record, transmit, or observe any events or listen to, record, or monitor any conversations which take place inside a subscriber's residence, workplace, or place of business. While §637.5(b) permits a video provider to compile, maintain, and distribute a list containing names and addresses of the its subscribers if the list contains no other individually identifiable information; and if the subscribers are afforded the right to elect to not (opt-out) to be included on such lists. SB1599 §637.5(b)

Subscribers would be afforded the right to elect to receive interactive services or technology allowing the video provider to collect, receive, aggregate, store or use electronic information regarding a subscriber's television viewing, without being denied video services by the video provider. SB1599 §637.5(f).

The bill also creates a civil cause of action, a violation of privacy, for any video provider who violates the section.

There is some ambiguity as to whether the author intends the subscriber to have to opt in or opt out

IV. European Union

A. European Union (EU) Directive on the Protection of Personal Data

The European Union (EU) Directive on the Protection of Personal Data (the Directive) (Council directive 95/46/EC, 1995 O.J. (L.281)) was enacted in 1995.

1. **Select Requirements of the Directive**
    a. Member countries must enact national laws to protect personal data (for status of national laws, see, next § IV.A.2);
    b. prohibited from restricting the free flow of data between member countries;

c. must restrict the flow of such data to nonmember countries whose laws do not "adequately" satisfy the Directive's standards;
d. all processing of data must be done "fairly and lawfully";
e. the purpose for which the data is collected must be specified and legitimate;
f. data must not be used for non-sanctioned purposes.;
g. the data collected must be relevant and not excessive in relation to the purpose;
h. personal data may only be processed upon the subject's specific, informed, and unambiguous consent;
i. exceptions to consent include:
    i. necessary to the performance of a contract;
    ii. to comply with a legal obligation;
    iii. to protect the vital interests of the subject;
    iv. in the public interest or in the exercise of official authority of the processing party; or
    v. in the legitimate interest of the processing party or third parties to whom the data has been disclosed.
j. the subject must be notified of the identity of the entity controlling the collection, the intended purpose of the collection, the third party recipients, when the collection is obligatory or voluntary, and the consequences of failing to provide information;
k. the subject must be given the right to access the data and to rectify incorrect information.
l. The subject must be given the right to object to the data being used for direct marketing; and
m. The data collected must be protected by a level of security appropriate to the risks presented and the nature of the data.[23]

2. Status of implementation of Directive 95/46[24]

Member State	State of play of legislative procedure	Next steps
Belgium	The implementation law was passed by the Parliament and published in the Official Journal of	

[23] J. Millstein, J. Neuburger & J. Weingart, Doing Business on the Internet: Forms and Analysis, §10.03[2]

[24] The European Union in the U.S., http://www.eurunion.org/partner/index.htm

Member State	State of play of legislative procedure	Next steps
	3 February 1999. Its entry into force is subject to secondary legislation that was published in December 1999.	
Denmark*	Partial implementation by a law amending the Civil Registration Act which came into force on 1 October 1998. Different bills introduced to the Parliament but not yet enacted.	Parliament to adopt a bill which was presented in December 1999.
Germany*	Formal bill yet to be presented. Parliamentary work yet to start. Legislation will be needed at the Laender level as well.	Parliamentary discussions likely to start in Spring 2000.
Spain	Implementation Law (Ley Orgánica 15/99) of 13 December 1999 came into force on January 14, 2000.	
France*	A bill is being considered by the Government.	Parliamentary discussions likely to start in Spring 2000.
Greece	Implemenation Law 2472 adopted on 10.4.1997.	
Italy	Law 675 of 31.12.1996 completed by secondary legislation.	
Ireland*	Draft bill presented to Government in July 1998.	Bill to be approved by Government and submitted to Parliament.
Luxembourg*	A draft bill has been finalised.	Bill to be approved by Government and submitted to Parliament.
The Netherlands*	Draft bill adopted by the Second Chamber on 23 November 1999.	Discussion and adoption by the First Chamber (Senate).
Austria	The Directive has been implemented by the Data Protection Act 2000 to enter into force January 1, 2000.	

Member State	State of play of legislative procedure	Next steps
Portugal	The Directive has been implemented by Law 67/98 of 26 October 1998.	
Sweden	Directive implemented by SFS 1998:204 of 29.4.1998 and Regulation SFS 1998:1191 of 3.9.1998, all of which came into force on 25 October 1998.	
Finland	The law was enacted by the Finnish Parliament on 10 February 1999 and entered into force on June 1, 1999.	
United Kingdom	The Data Protection Act 1998 received Royal Assent on 16 July 1998. Secondary legislation has been adopted and the Act entered into force on 1st March 2000.	

*) This means that the Member State is being sued before the European Court of Justice for failure to notify the implementing measures within the deadline established by the Directive.